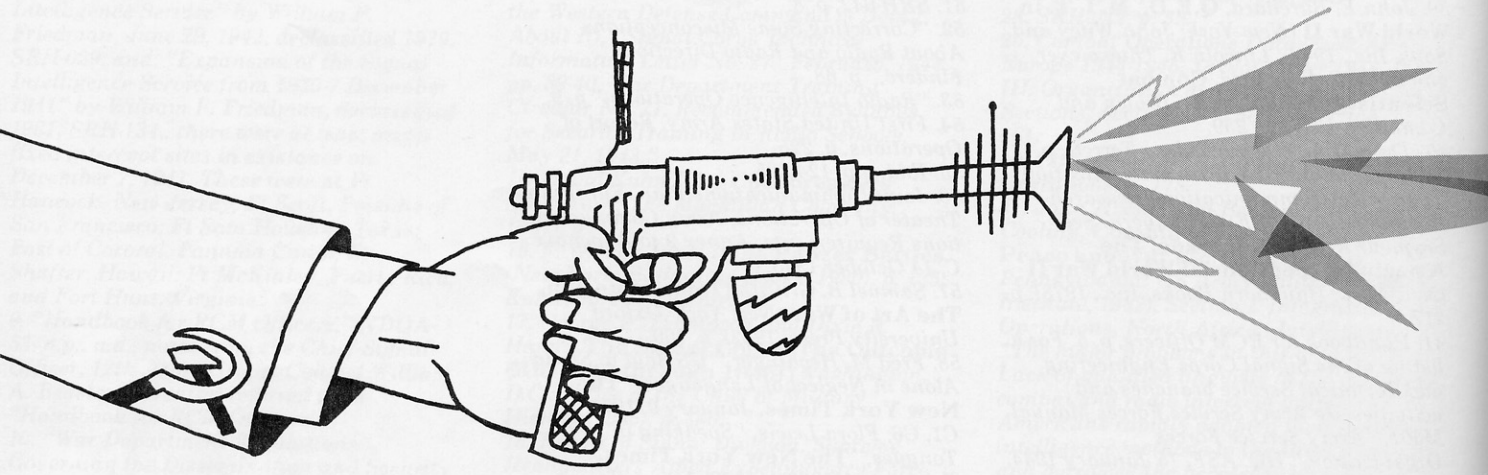
New perspectives on Electronic



It appears that most of the electronic warfare terms that are usually taught as unrelated concepts of ECM, ESM and ECCM can be integrated...

by Capt. Walter R. Schumm

The U.S. Army's concern with overcoming the threat of Soviet radio-electronic combat is exemplified in recent publications such as Training Circular 30-22, *Battlefield Survival and Radioelectronic Combat* (July 1978) and articles such as one by Maj. Barney F. Slayton, "War in the ether: Soviet radioelectronic combat," which appeared first in *Military Review* and was reprinted in *The Army Communicator*. Unfortunately, the ideas which appear in such resources too often fail to integrate what we know about electronic warfare defense in ways that facilitate training in either a school environment or in the field.

In the classroom, electronic warfare training usually begins with a laundry list of spaghetti soup terms that convinces trainees that the rest of the afternoon is going to be a tough one to stay awake in. The line and block charts that can be generated explaining and differentiating terms such as ELINT, TELINT, SIGINT, EW, ESM, ECM, ECCM, COMINT, SIGSEC, ELSEC and REC among others are nothing short of amazing for their effectiveness as an agent of confusion and somnolence.

Warfare defense

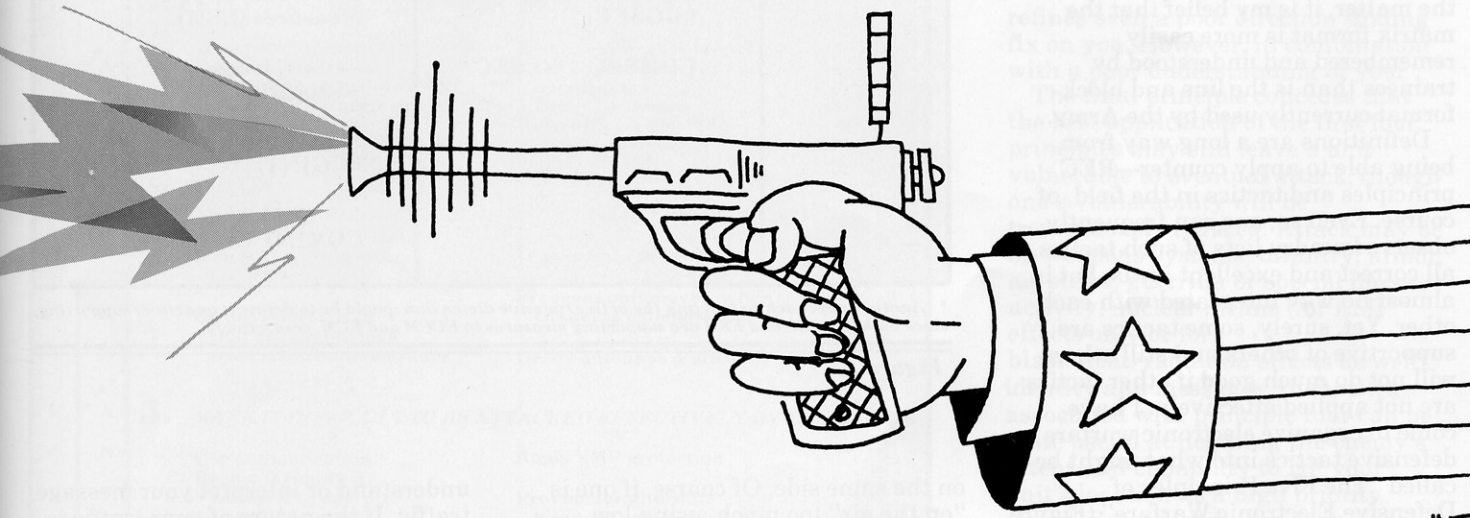


illustration by Ronald Altizer

One of my father's professors at the Naval Academy (circa 1925) used to say that if you couldn't draw a picture of it you probably didn't understand the concept in question. Oftentimes it really does help to try to get away from line and block charts and try other approaches to illustrating how concepts are interrelated. What follows is the result of such an attempt in the realm of electronic warfare defensive measures, which has proved useful to me for getting across ways in which EW terms and practices are interrelated.

It appears that most of the electronic warfare terms that are usually taught as unrelated concepts of ECM, ESM, and ECCM can be integrated as shown in Figure 1, a four-cell matrix in which every cell can be related in a meaningful way to its adjacent neighbor. The terms electronic support measures (ESM) and electronic countermeasures (ECM) are clearly offensive aspects of electronic warfare (EW), as electronic countermeasures (ECCM) and signal security (SIGSEC) are clearly defensive measures. Moreover, signal security (SIGSEC) and electronic support measures (ESM) are relatively passive measures that, if ignored, will tend to negate the effectiveness of their counterparts, electronic counter-countermeasures (ECCM) and electronic countermeasures (ECM), which are more active measures adopted to directly attack or defend against a direct attack by the enemy. The cell for ESM is divided into two components: ESM (measures that gain information important for conducting ECM) and SIGINT (intelligence used for tactical or strategic operations of a wider scope than ECM by themselves). The dashed line between ESM and SIGINT is used to indicate that some of the information for each concept is the same—frequencies, unit locates, unit identities, for example.

In the Soviet concept, one might imagine that they would substitute radioelectronic combat (REC) for the ECM cell and a wider concept of the defense where we have put ECCM.

For instructional purposes, one can ask students to explain the relationships between the cells, which is easily done upon a little bit of reflection or one can explain the relationships directly. SIGSEC, for example, is a form of counter-SIGINT or anti-ESM, depending on which prefix one wishes to use. It is also an important foundation for ECCM, which can only remediate a bad situation that has been allowed to develop, in most cases, because poor SIGSEC allowed the enemy to develop ESM adequate for conducting effective ECM. ECCMs, likewise, are counter-ECM practices that depend on their effectiveness for previous and current SIGSEC practices. Similarly, ECMs depend on effective ESM and both ESM/SIGINT and ECM are intended to operate against the SIGSEC and ECCM of enemy units.

	DEFENSIVE	OFFENSIVE
ACTIVE	Electronic Counter-Counter Measures (ECCM)	Electronic Counter-Measures (ECM) Jamming Imitative Communications Deception (ICD)
PASSIVE*	Signal Security (SIGSEC) COMSEC ELSEC	Electronic Support Measures (ESM) - - unit, freqs - - - - location - - Signal Intelligence (SIGINT) COMINT ELINT TELINT

** Another approach to labeling the active/passive dimension would be to define it as active/supporting, since both SIGSEC and ESM are supporting measures to ECCM and ECM, respectively.*

Figure 1.

Although I have not done research on the matter, it is my belief that the matrix format is more easily remembered and understood by trainees than is the line and block format currently used by the Army.

Definitions are a long way from being able to apply counter—REC principles and tactics in the field, of course. Even so, one can frequently observe laundry lists of such tactics, all correct and excellent ideas, but in almost no way integrated with each other. Yet, surely, some tactics are supportive of others and still others will not do much good if other tactics are not applied effectively. I have come to organize electronic warfare defensive tactics into what might be called "The Five Principles of Defensive Electronic Warfare" (Figure 2).

The first principle refers to minimizing one's use of the radio. In fact, if one never used a radio at all, the subsequent four principles would become largely irrelevant and unnecessary. Of course, there is not much use having a radio transmitter if it is never turned "on the air." As with all of the five principles, the application of this principle will never be perfect; the objective is rather to operate in such a manner as to make the enemy's job so difficult as to afford maximum protection for one's unit and one's ability to keep communicating securely. The specific tactics listed under each principle are only a few of the possible things that can be done and are identified for illustration rather than as an attempt to include all possible techniques.

The second principle acknowledges that transmissions will be taking place. However, it is desirable to minimize radiation distances and patterns, especially in the direction of enemy ground based or airborne COMINT units, across the FEBA or on the same side. Of course, if one is "on the air" too much, using low power or terrain masking will help but not nearly as much as if transmissions are minimized. Some techniques such as the use of horizontally polarized field expedient antennas may be an asset for minimizing the chances of being intercepted and fixed by direction finding in certain terrain, but in heavily wooded terrain where a lot of forest is between one and the enemy, the use of vertically polarized antennas might lead to a greater absorption of signal by the trees before it reaches the enemy ground-based stations.

The third principle recognizes that the enemy will probably intercept some transmissions. However, what he does with that information will depend on the degree to which he can understand or interpret your message traffic. If the nature of your traffic is such that he thinks it represents the communications link of a nuclear-capable artillery unit, it will probably receive a higher priority than something he thinks is from a supply and service company. The use of speech secure equipment by itself would serve to protect much of a unit's identity unless, of course, such equipment is limited to a very few units. Assuming that not all units will have secure equipment for some time and that those which do will experience some degree of equipment malfunctioning (for maintenance reasons or because of enemy jamming), other tactics assume no small degree of significance. One procedure, of substantial controversy, is the use of highly trained radio operators rather than anyone who can key a microphone as the only legitimate operators of communications equipment. In my own tactical experience, the higher the rank of the radio user, the greater the tendency for that user to assume he has the

SIGSEC — ANTI-SIGINT / ANTI-ESM

1. *MINIMIZE TIME "ON THE AIR"*

- Direct (don't staff) the battle by radio
- Think/write it down/ then transmit
- Preplanning & briefings
- Use alternate means of communication
- Burst transmissions
- Brevity codes
- Abbreviated callsigns
- Keep transmissions brief
- Eliminate all non-essential traffic

2. *MINIMIZE RADIATION PATTERNS*

- Terrain masking
- Use directional antennas
- Operate on low power
- Reduce antenna height
- Use horizontally polarized antennas
- Use dummy antennas for tuning

3. *MAKE YOUR IDENTIFICATION DIFFICULT FOR THE ENEMY*

- Use speech secure gear
- Use standard radio-telephone procedures
- Use and rotate among units radio operators
- Integrate other OPSEC procedures w/SIGSEC
- Encrypt messages properly
- Change CEOI periods and operations at irregular times
- Keep officers and other careless personnel off the "air"

4. *MAKE IT DIFFICULT FOR THE ENEMY TO FIX YOUR LOCATION*

- Remote your radios and antennas
- Do not select CP sites that are too obvious from map reconnaissance
- Transmit on the move
- Frequent unit moves; when changing callsigns.
- Decoy antennas & sites

5. *MAKE IT DIFFICULT TO BE ATTACKED EFFECTIVELY BY THE ENEMY*

- Use authentication
- Report jamming & continue to operate
- Take/construct good cover against artillery or missile attack
- Know when and how to change frequency in order to minimize its compromise
- Apply EMP protection
- Provide for alternate means of communication in emergencies
- Apply proper camouflage procedures
- Coordinate defenses and emergency communications with other units

ECCM — ANTI-REC

Figure 2.

privilege of violating all manner of communications security procedures; unfortunately, there are entirely too many possible rationalizations available (which may be valid in some situations) for ignoring communications security: enemy inability to conduct SIGINT operations, importance of tactical mobility and speed, and personal inconvenience. On the latter point, which may seem unnecessary, I must point out that many times as a junior officer my attempts to enforce SIGSEC procedures were directly countermanded by field grade officers who insisted flat out that their personal convenience was more important than any tactical advantage that might be gained from good signal security. I would prefer to see radio operation limited to highly trained enlisted operators who could be rotated among units to negate any enemy attempts at voice fingerprinting or the identification of any other unusual operator characteristics.

The fourth principle will do little good if one's unit violates the first three principles because it will only be a matter of time before the enemy refines even a poor direction finding fix on you. However, in combination with a poor understanding of your

The final principle concedes that the best application of the first four principles may still leave a unit vulnerable to eventual attack, though one's vulnerability will be tremendously reduced. Attack may be by weapons systems, infantry, armor, air strike, guerrilla or special forces activity, nuclear means (for EMP effects only or for blast/heat/radiation effects as well), identity and messages, the tactics associated with principle four can be quite useful at negating the enemy's intent and capability to DF your unit's location as a high priority target. Some techniques such as remoting antennas should not be done so much as to make the fix difficult but to further confuse the enemy as to the type of unit putting out such a different radio signature or overall electromagnetic profile. If one transmitted infrequently, one intriguing approach to defeating DF attempts would be to send messages by jeep some distance from the unit and have them sent while the jeep was moving at high speed; of course, one should site such movements for the best terrain masking and in patterns that do not suggest your unit's actual location. Some techniques, such as changing callsigns and frequencies, are not too effective if your unit stays in the same place before and after the change (of course, not every unit should try to move when callsigns are changed because of the excessive confusion that would be created). One has to remember that the Soviets, in spite of their artillery trigger-fingers, will still likely look at a map in order to refine their DF-acquired targets; thus, choosing an obvious site on the map will only assist them in their efforts to pinpoint your location from an otherwise very rough DF fix.

jamming, or imitative deception and net intrusion. While prevention is worth several cures, it is still important to know what to do when attacked by radioelectronic combat related means.

The arrangement of the five principles in an interdependent hierarchical order leads us to several important implications for defensive EW training. First, the need to reiterate that prevention cannot be overemphasized by giving priority to signal security, anti-SIGINT, anti-ESM tactics over ECCM or anti-REC tactics. Only if one concludes that the command emphasis within one's unit is inadequate to support or sustain such an emphasis should one switch to an emphasis on ECCM tactics. Secondly, use of the five principles can assist in the evaluation of a unit's overall operational security, breakdowns in which can be pinpointed at the most appropriate level rather than perhaps focusing on the third principle when in fact violations of the first or second principle were primarily responsible for tactical losses. The results of such analyses should be fed back into the training plan with emphasis on training in, for example, the second principle over the third principle, everything else being equal. Finally, within each level, one can analyze for each given tactical environment or situation, which particular techniques would be most feasible to employ and which ones of those that were feasible would be most effective at denying the enemy what he needs to know in order to conduct effective radioelectronic combat attacks against us. However, the primary advantage of the principles and their integration as shown in Figure 2 is that what was once a laundry list of unrelated, hit or miss, catch-as-catch-can ideas has been redefined into a format that allows a more rapid and efficient analysis of any given EW defensive situation, in either the classroom or in the field environment.

ENDNOTE

In Figure 2, the left border is divided to indicate the correspondence between each principle and SIGSEC/ECCM and anti-SIGINT/ESM/REC tactics. The slanted, dotted lines between anti-SIGINT, anti-ESM, and anti-REC concepts indicate the overlap between the principles in their application in EW defense.

Capt. Schumm is an assistant transportation movement control officer with the 425th Transportaiton Center (MC), 89th U.S. Army Reserve Command and Senior Instructor, Electronic Warfare Committee, 6th United States Army Intelligence Training Army Area School. He has served on active duty with the 1st Infantry Division and in a variety of staff and unit command positions with Signal units in the Kansas and Indiana Army National Guard. He is an associate professor of family studies at Kansas State University and has a secondary specialization as a Health Services Research Psychologist (SSI 68T) in the Army Reserve. Schumm is a 1972 graduate of the Reserve Officer Training Corps program at the College of William and Mary in Virginia.

Schumm is a 1972 graduate of SOBC (Honor Graduate) and an Honor Graduate of the 1973 class of C/E Staff Officers Course at Fort Sill. He has served as the C/E Officer for HHD, Kansas Army National Guard Commander of the 135th Signal Platoon, 69th Infantry Brigade, Kan ARNG, as well as Commander, "B" Company, 138th Signal Battalion, Ind ARNG and Radio Officer, 38th Infantry Division, Ind ARNG. On active duty, he served in the 121st Signal Battalion, 1st Infantry Division and in the 1/5th Field Artillery as their Communications Platoon Leader. He has also completed the Signal Officers Advanced Course (correspondence).